

REMARKS

The Office Action of November 5, 2004 has been reviewed and the Examiner's comments carefully considered. The present Amendment amends claims 1-7, 9, 11, 14, 17, 20, 22 in accordance with the originally-filed specification. Support for these amendments can be found, for example, on page 18, lines 5-6 and top of page 22 of the originally-filed specification. No new matter has been added. Claims 1-23 remain pending in this application.

Objections to the Specification

In the specification, the Abstract has been amended to address the Examiner's objections and to avoid phraseology such as "means" and "said". Reconsideration of this objection is respectfully requested.

Objections to the Drawings

The drawings stand objected to for failing to comply with 37 CFR 1.84(p)(5) because they did not include a reference sign mentioned in the description: "cryptographic engine 30". In addition, the drawings stand objected to for failing to comply with 37 CFR 1.84(p)(4) because reference characters "10, 12, 14, 16" appear to point to the same part in the drawing. A drawing sheet showing a proposed drawing correction to Fig. 1 in red ink and a replacement sheet having Figs. 1-2 with the correction are enclosed herewith. The Applicant believes that new Fig. 1 overcomes the Examiner's objections. Reconsideration of these objections is respectfully requested.

Claim Rejections

Claims 2-7, 20, and 22 stand rejected under 35 U.S.C. § 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which Applicant regards as the invention. Specifically, the Examiner rejects claims 2-7, 20, and 22 as including terms and limitations that have insufficient antecedent basis. Claims 2-7, 20, and 22 have been modified to overcome this rejection. Therefore, withdrawal of the Examiner's indefiniteness rejections of claims 2-7, 20, and 22 is respectfully requested.

Claims 1, 4, 10, 12-13, and 17-23 stand rejected under 35 U.S.C. § 102(e) as being anticipated by U.S. Patent No. 5,917,913 to Wang. Claims 2, 3, 5, and 14-16 stand rejected under 35 U.S.C. § 103(a) as being obvious over the Wang patent in view of Bruce Schneier, *Applied Cryptography*, 1996, John Wiley & Sons, Second Edition, Pages 43-44. Finally, claims 6, 7, 8, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being obvious over the Wang patent in view of U.S. Patent No. 6,408,388 to Fisher.

Independent claim 1 of the present application, as amended, is directed to a digital private key protection device for securely storing a user's digital private key and digitally signing received data. The digital private key protection device includes a cryptographic engine, a communications port, a user operable input and a trusted display. The communications port is for receiving and transmitting to an external device. The user operable input is connected to the cryptographic engine such that the user can communicate approval of a displayed message when deemed trustworthy. If the user operable input is operated, the cryptographic engine applies the user's digital private key in order to digitally sign the data and then transmits the data externally via the communications port of the digital private key protection device.

The Wang patent, the primary reference in all of the prior art rejections, is directed to a portable electronic authorization device (PEAD) that performs a method for approving transaction requests originated from an electronic transaction system. The method disclosed in the Wang patent includes receiving digital data at the device and using the device to approve the digital data, which generally includes transaction details. The method further includes using a stored and protected PEAD user key to encrypt and sign the received digital data to signify approval of the transaction details.

The present invention, as defined in the claims of the present application, is distinguishable from the PEAD device of the Wang patent and the remaining prior art of record. In particular and as specifically set forth in independent claim 1, the digital private key protection device of the present invention includes a trusted display. Therefore, the present invention assumes that all displays not under its control are untrusted displays and subject to the threats disclosed in the specification. For a practical example very common on the internet recently, in an endpoint attack in which an attacker alters software on a sender's computer, an untrusted display is vulnerable since it could display the transaction incorrectly and result in a signature being applied to an unintended transaction. The present digital

private key protection device provides protection against this scenario by providing the best possible and most trustworthy means for the user to acquaint themselves with the actual details of received transactions. This protection is assured since the user of the PKPD of the present invention must review the transaction through the trusted display, after which and only then the user must deliberately elect to authorize the transaction.

Applicant respectfully submits that the Wang patent makes no disclosure of this critical characteristic of Applicant's invention. At column 10, line 66 the Wang patent states: "Optional display 610 may be implemented...Displays (sic), 610 displays, among others, the transaction being proposed for approval. Display 610 may be omitted if desired, in which case the transaction may be viewed, for example, at a display associated with the electronic transaction system itself." An untrusted display could display the transaction incorrectly. The Wang patent teaches away from a trusted display as shown in the citations above with the term "optional" and the omission if desired and inclusion of a display merely associated with the electronic transaction system and not the PEAD.

Accordingly, in an e-commerce scenario where a user of a PEAD of the Wang patent might rightly expect that an internet transaction displayed on a PEAD display (or on the transaction system screen, since Wang PEAD display is optional), is a payment of \$29.95 to Amazon.com, it may not be. In the Wang PEAD, it is likely that an associated display on a Web page may even suggest or reinforce that expectation. However, the real transaction may not match the displayed transaction in the Wang untrusted display and the transaction may in fact be a transaction that transfers \$29.95 to an unintended recipient, such as a cyber criminal. Using the Wang PEAD would result in the user's digital signature being applied to the spoofed transaction. The signature of the Wang patent relates to the receiver of the message that the user has authorized this transaction. In addition, the PEAD authorization relates to the transaction receiver that the current transaction has been authorized and in contrast to the typical e-commerce transaction authorization, in this one the authorizer has elected to use his own special private key to witness the authorization of the transaction. The PEAD authorization further relates that the possibility that someone else has used the authorizer's keys is substantially minimized by the PEAD security functionality. Finally, the authorization relates that PEAD security functionality has been evaluated and certified by security authorities to be sufficiently trustworthy for the present application. Clearly, it will

be difficult for the authorizer to repudiate the transaction of paying \$29.95 to a cyber criminal, when he has most assuredly authorized it.

This problem, now known as Phishing, is addressed by the present invention's trusted display. A user is able to authorize a transaction only after reviewing information displayed on the trusted display, at which point his authorization causes the signature to be applied to the transaction. This means that the signature can be interpreted (perhaps by a court) not only with the meaning above from the Wang example but with the additional and more important meaning that the user has deliberately authorized this specific transaction and only after being made fully aware of the content of the transaction. Furthermore, it relates that the possibility of the user's signature being applied to an incorrect document has been minimized by use of the trusted Private Key Protection Device (PKPD) security functionality. In this case, if the transaction to be authorized was actually to transfer money to Amazon, the authorizer would very likely approve it. However, if the transaction was supposed to transfer money to a cyber criminal, then the authorizer would have seen this detail on the trusted display and made a judgment not to authorize it.

The PKPD of the present invention is shown to provide a novel and much stronger signature. It indicates not only the authenticity and the integrity of the message but it also assures the receiver that the authorizer made a deliberate and informed choice to sign the document that was being transmitted. PKPD assures that the proper transaction is authorized. Most would agree that it is important not to sign a document without reading and understanding the contents of that document, yet without a trusted display, that is precisely what the PEAD allows.

Wang recognizes a number of security threats that might apply to private keys held on smart cards, swipe cards, or computers in its "background to the invention" and recognizes that computers are vulnerable to certain threats. However, what the Wang patent fails to recognize is the threat that a computer might display an incorrect document that attempts to induce a person to sign or authorize a transaction, which is becoming a major problem. During the year 2004 and into 2005, there were enormous increases of this type of Phishing activity. Information purporting to be from Banks, Microsoft, or other reputable institutions request a user to click on a link to a website or enter a PIN number to engage in a transaction. The perceived transactions are only present to deceive a user in order to draw the user to a website and then fraudulently transact data entirely different from what the user

expected and as shown above, the Wang PEAD would be of no assistance in these types of circumstance.

For the foregoing reasons, independent claim 1 is not anticipated by or rendered obvious over the Wang patent. In addition, none of the Wang patent, the Fischer patent, the Schneier publication, nor any of the prior art of record, whether used alone or in combination, teaches or suggests a digital private key protection device that includes a trusted display as set forth in independent claim 1 of the presently amended application. Therefore, reconsideration of the rejections of independent claim 1 is respectfully requested. Since claims 2-23 depend either directly or indirectly from, and add further limitations to, independent claim 1, these claims are also believed to be allowable for the reasons discussed hereinabove in connection with independent claim 1.

Claims 2, 3, 5, and 14-16 stand rejected under 35 U.S.C. § 103(a) as being obvious over the Wang patent in view of Bruce Schneier, *Applied Cryptography*, 1996, John Wiley & Sons, Second Edition, Pages 43-44. The Schneier publication teaches signing public keys with a trusted private key for each encryption and decryption operation. In other words, the process of verifying signatures using public key cryptography. This method is well known in the art and is not what is being claimed in the present application. Instead, with regards to claim 2, the present application claims to improve the trustworthiness of the verification calculations and the subsequent display of the results of the verification calculations. Display of the verification results on a trusted display thereby eliminates any risk that the verification results could be untrustworthy. The Wang patent does not provide for the trusted display of such verification results nor does Schneier teach that it is necessary or appropriate to perform these operations on a device which is not vulnerable to all the threats under consideration.

For the foregoing reasons, claim 2 is believed to be allowable. None of the Wang patent, the Schneier publication, nor any of the prior art of record, whether used alone or in combination, teaches or suggests a digital private key protection device that includes a trusted display as set forth in claim 2 of the present application. Since claim 5 depends directly from, and adds further limitations to, claim 2, claim 5 is believed to be allowable for the reasons discussed hereinabove in connection with claim 2. Reconsideration of the rejections of claims 2 and 5 is respectfully requested.

With regards to claim 14, the present application discloses a PKPD device containing a digital shared secret symmetric key. This is different than the public key cryptography taught in the Schneier publication which utilizes public and private key pair combinations.

Finally, claims 6, 7, 8, 9, and 11 stand rejected under 35 U.S.C. § 103(a) as being obvious over the Wang patent in view of U.S. Patent No. 6,408,388 to Fischer. The Fischer patent teaches a device providing trusted timestamps. The reader includes a device for storing on a smart card reader a private key used in performing a digital signature operation. The device receives information indicative of at least one of date and time from a source, i.e., a computer, for performing a digital signature operation with the private key for output.

However, although it is critical to protect the private key used for creating these timestamps, in this situation there is no need to take care about what documents the timestamp is applied. The semantics of the timestamp merely indicate that the attached document existed at 7:43 p.m. on February 24, 2005. Validation of the document may never occur under the Fischer patent. The timestamp does not mean that the authorizer read and agreed with the attached document at 7:43 p.m. on February 24, 2005. Because of the smaller semantic imputed by the timestamp signature, it is not critical to ensure that the timestamp signer views each document before applying the signature. This is in stark contrast to claim 6 of the present invention where it is critical for someone applying a personal signature, used to authorize a transaction or affirm a military order, to read the information contained in the document being signed. The trusted display element of the present application is therefore critical.

For the foregoing reasons, claim 6 is believed to be allowable. Since none of the Wang patent, the Fischer patent, nor any of the prior art of record, whether used alone or in combination, teaches or suggests a digital private key protection device that includes verification of received digital data which has been encrypted by a private key protection device. In fact, the Fischer patent teaches away from claim 6, since the nature of a timestamp negates the criticality of viewing and therefore validating each document before application of the signature. Reconsideration of the rejection of claim 6 is, therefore, respectfully requested.

Next, with regards to claim 7 of the present application, the Fischer patent does not disclose decrypting received data nor using its own or another device's public key to do so. More importantly, claim 7 is directed to verification of received digital data which has been encrypted by a private key protection device and the Fischer patent does not disclose this requirement, contrary to the words of the Examiner. In the words of the Examiner relating to

claim 7 “a modification would have been obvious to one of ordinary skill in the art of cryptography to encrypt with either public key or private key to verify a corresponding key,” however, claim 7 is directed to decryption not encryption.

For the foregoing reasons, claim 7 is believed to be allowable. None of the Wang patent, the Fischer patent, nor any of the prior art of record, whether used alone or in combination, teaches or suggests a digital private key protection device that includes verification of received digital data which has been encrypted by a private key protection device. Since claim 8 depends directly from, and adds further limitations to, claim 7, claim 8 is also believed to be allowable for the reasons discussed hereinabove in connection with claim 7. Reconsideration of the rejections of claims 7 and 8 is, therefore, respectfully requested.

With regard to claim 11, Applicant respectfully disagrees that the Wang patent teaches one to use the Wang PEAD for decryption of received digital data. The Wang patent claims a PEAD device that is used primarily as an authenticator. Moreover, the primary function of the PEAD device of the Wang patent is to receive transactions provided by a third party and subsequently to authenticate the transactions. Wang teaches authentication of transactions through the use of a user's private key, it does not extend to teach or suggest a PEAD that decrypts using a user's private key. To assume that the Wang PEAD decrypts, and likewise inferring that received transactional data has been encrypted by the user's public key prior to receipt, is much too tenuous. The usage of the Wang PEAD in such a manner as described above strays far from the teachings of the Wang patent. However, claim 11 has been amended to include the limitation that a decrypted transaction is not released until a user operable input means has been operated. Therefore, to extend the Wang application to disclose a PEAD for use by a user operable input for the function of enabling a decryption function when the PEAD of Wang is primarily an authenticator and encryption device is impermissible. For the foregoing reasons, claim 11 is believed to be allowable. Reconsideration of the rejection of claim 11 is respectfully requested.

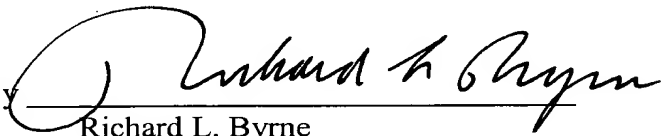
Application No. 09/856,813
Paper Dated March 7, 2005
In Reply to USPTO Correspondence of November 5, 2004
Attorney Docket No. 1376-010862

Conclusion

For all the foregoing reasons, Applicant believes that claims 1-23, as amended, are patentable over the cited prior art and in condition for allowance. Reconsideration of the rejections and allowance of all pending claims 1-23 are respectfully requested.

Respectfully submitted,

WEBB ZIESENHEIM LOGSDON
ORKIN & HANSON, P.C.

By 

Richard L. Byrne
Registration No. 28,498
Attorney for Applicant
700 Koppers Building
436 Seventh Avenue
Pittsburgh, Pennsylvania 15219-1818
Telephone: 412-471-8815
Facsimile: 412-471-4094
E-mail: webblaw@webblaw.com

Application No. 09/856,813
Paper Dated March 7, 2005
In Reply to USPTO Correspondence of November 5, 2004
Attorney Docket No. 1376-010862

AMENDMENTS TO THE DRAWINGS

The attached sheet of drawings includes a proposed drawing correction to Fig. 1 in red ink. This sheet, which includes Figs. 1 and 2, replaces the original sheet including Figs. 1 and 2. In Fig. 1, previously omitted element 30 has been added. Approval of the proposed drawing correction is respectfully requested.

Attachment: Replacement Sheet
Annotated Sheet Showing Changes

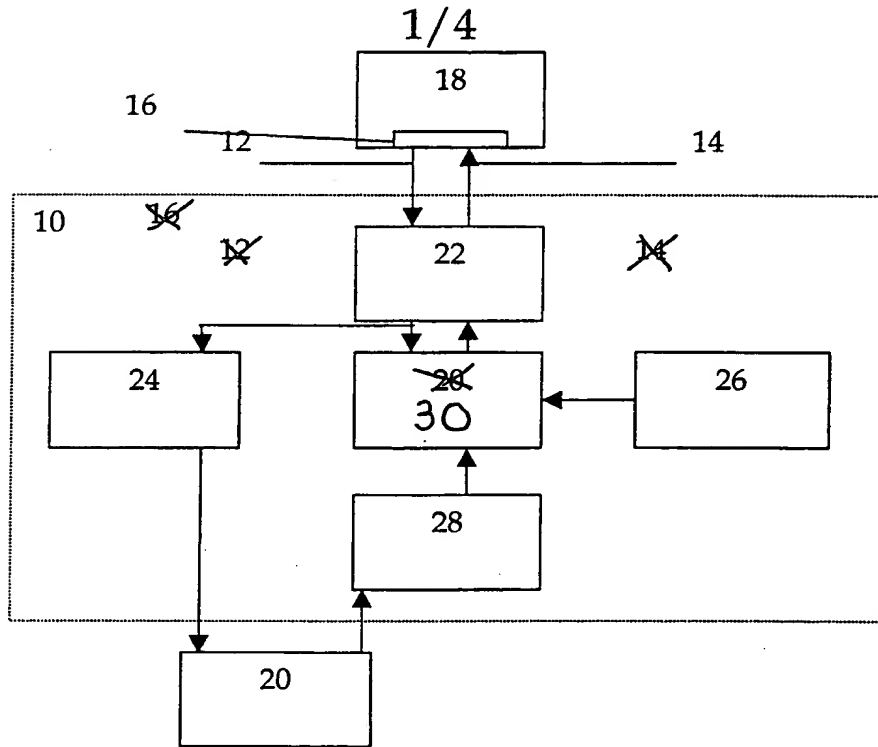


FIG. 1

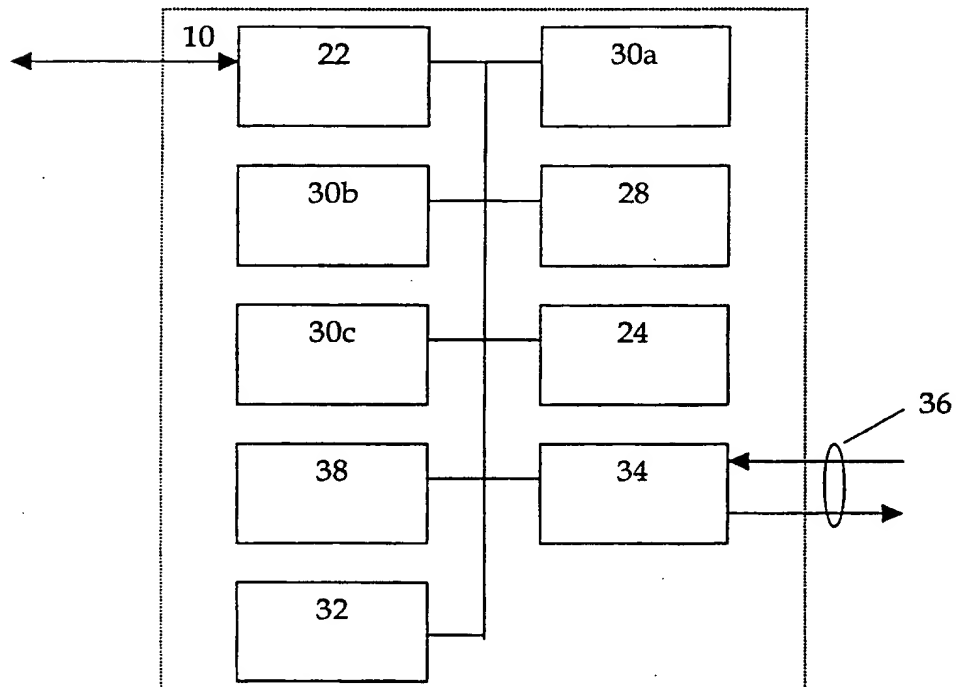


FIG. 2